Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
Swiss Government Computer Emergency Response Team (GovCERT.ch)

Cyberbedrohungen und der Schutz des Wirtschaftsstandort Schweiz

20. September 2022

Themen

Referenten:
- **Roman Hüssy**
  Technischer Analytiker Cybersicherheit

1	**Das Nationale Zentrum für Cybersicherheit**
2	**Wie das NCSC Informationen beschafft**
3	**Wie das NCSC Informationen verwendet**
4	**Fragen**

1. Das Nationale Zentrum für Cybersicherheit

Das Nationale Zentrum für Cybersicherheit

- Ist das Kompetenzzentrum des Bundes im Fachbereich Cybersicherheit
- Ist Anlaufstelle bei Thema Cybersicherheit für:
  - Wirtschaftsstandort Schweiz
  - Kritischen Infrastrukturen
  - Öffentliche Verwaltung
  - Hochschulen
  - Öffentlichkeit
- Ist zuständig für die koordinierte Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS)
- Kernauftrag: Schutz der kritischen Infrastrukturen in der Schweiz (KRITIS) vor Cyberbedrohungen

Das Nationale Zentrum für Cybersicherheit

- Unterstützt **subsidiär** beim Schutz vor Cyberbedrohungen sowie bei der Bewältigung von Cybervorfällen
- Hat **keine Weisungsbefugnisse** gegenüber Dritten, sondern gibt **Empfehlungen** ab

Cyber-Sicherheit	Cyber-Strafverfolgung	Cyber-Defence
Schutz vor Cyberbedrohungen und Bewältigung von Cybervorfällen	Verfolgung von Straftaten im Cyber-Raum	Verteidigung des Cyber-Raums bei kriegerischen Handlungen
> NCSC.ch	**> Strafverfolgungsbehörden** (Kantone, Bund)	**> VBS (Armee)**

Das Nationale Zentrum für Cybersicherheit

Beobachtung Cyberbedrohungen	Alarmieren	Technische Analysen	Entwicklung von Tools und neuen Dienstleistungen	Incident Response
IKT-Vorgaben Bund	Sensibilisierung und Awareness	Koordination Umsetzung NCS	Schwachstellen-Management	Beratung bei Erarbeitung regulatorischer Vorgaben

2. Wie das NCSC Informationen beschafft

Wie das NCSC Informationen beschafft

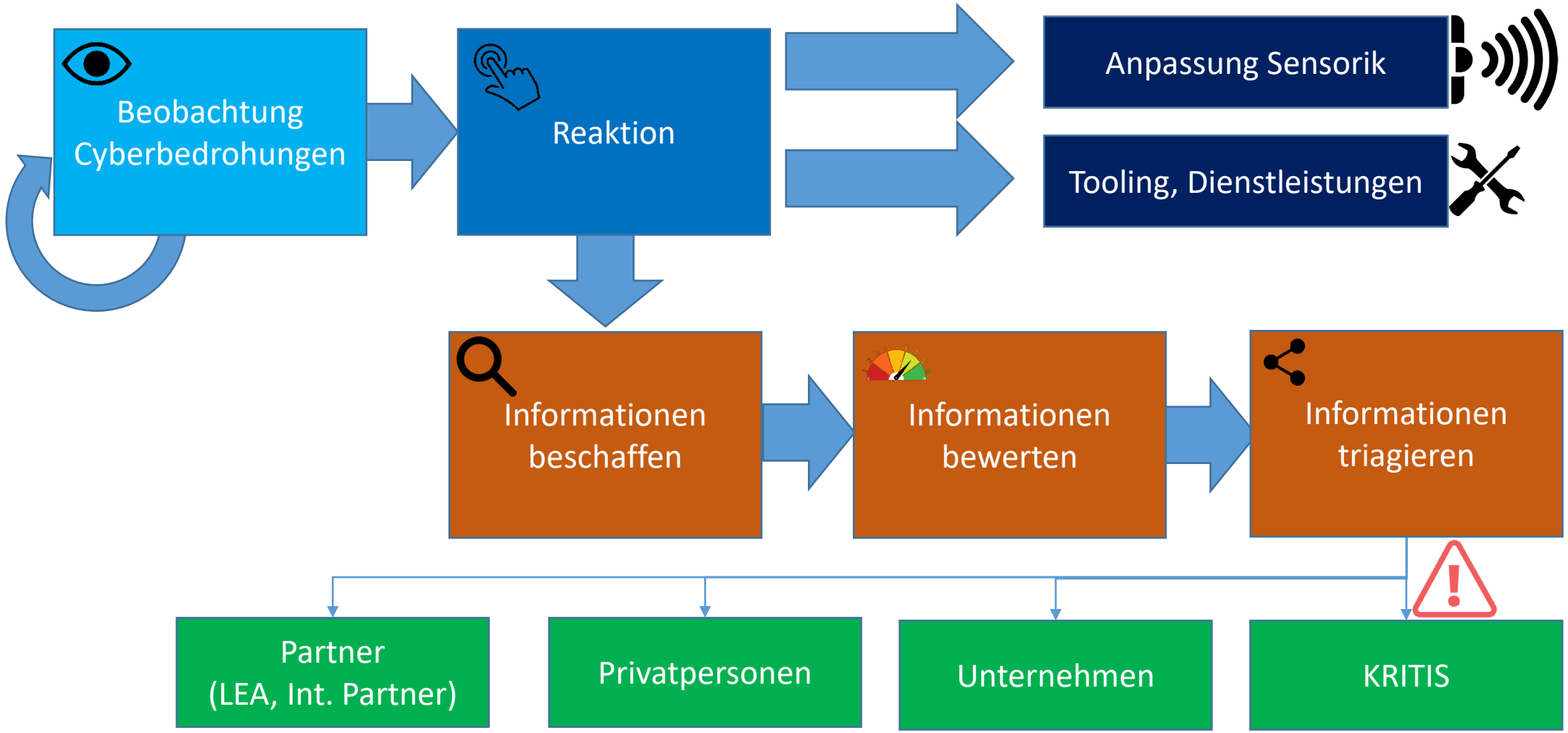
- Das Internet kennt keine Grenzen: Viele Cyberbedrohungen betreffen alle
  - ➢ **Nationaler Austausch** mit KRITIS
  - ➢ **Internationaler Austausch** mit «like-minded» Staaten und Organisationen
- Sammeln von Informationen aus **öffentlich zugänglichen Quelle (OSINT)**
- Sammeln von Informationen aus **eigener Sensorik**

Wie das NCSC Informationen beschafft

- Welche Information beschafft das NCSC?
  - **Kontextualisierte**, **technische** Informationen zu Cyberbedrohungen («Cyber Threat Intelligence» - kurz **CTI**)
  - Modus-Operandi von Akteuren

- z.B:
  - «Die Webseite **X** wird aktuell für die Verbreitung der Malware **Y** verwendet»
  - «Der Domain-Name **Z** wird aktuell für die Steuerung von mit der Malware **Y** infizierten Geräten verwendet»
  - «Akteur **X** verwendet die Technologie **Y** zur Umgehung von 2FA»

Wie das NCSC Informationen beschafft



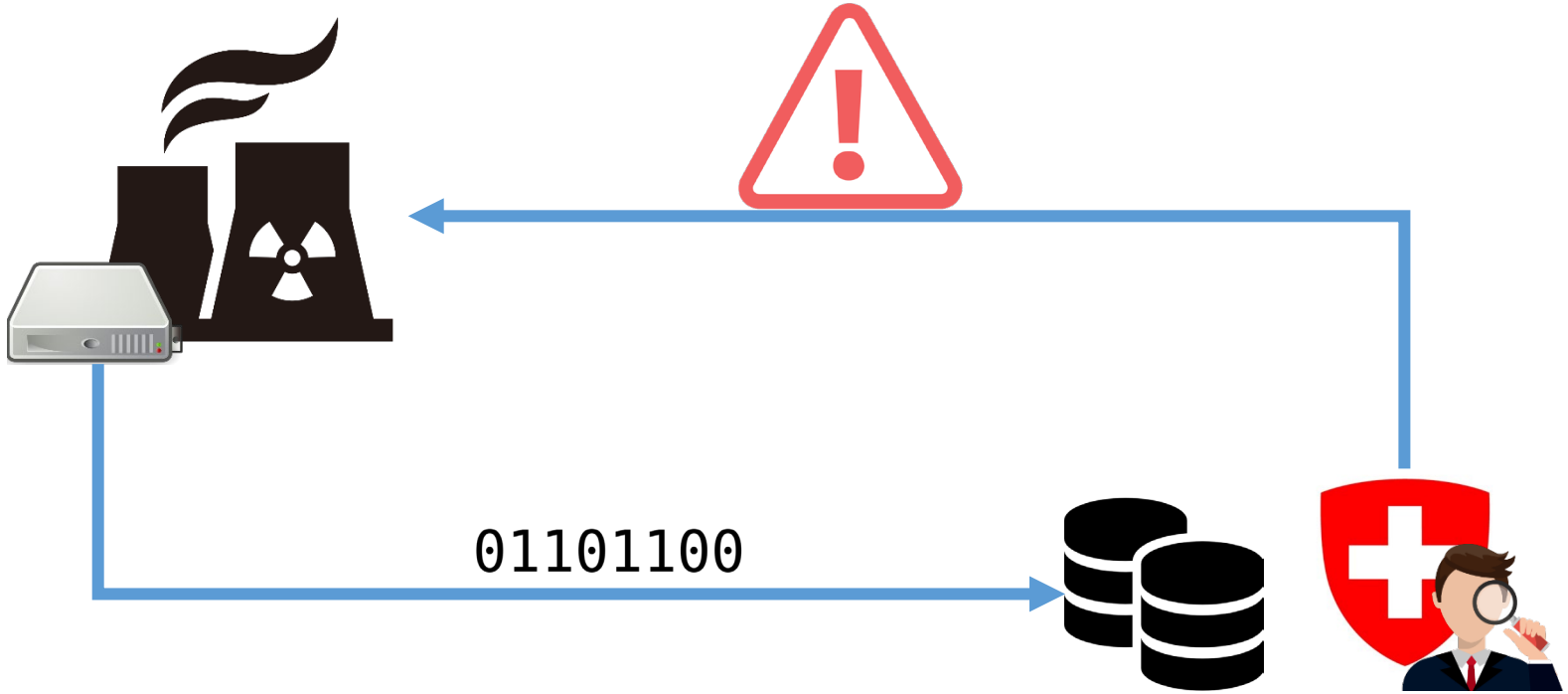
Wie das NCSC Informationen beschafft

- Agilität durch Inhousing:
  - ➢ Betrieb **eigener Infrastruktur** ermöglicht es **zeitnah** auf Cyberbedrohungen zu reagieren und z.B. innert weniger Tagen entsprechende **Tools zu entwickeln und zur Verfügung zu stellen**

- Eigenentwicklung und Open-Source:
  - ➢ Wir setzen grösstenteils auf Eigenentwicklungen und Open-Source Tools, was wiederum unsere Agilität fördert

Wie das NCSC Informationen beschafft

- Beispiel Funktionsweise Sensorik



3. Wie das NCSC Informationen verwendet

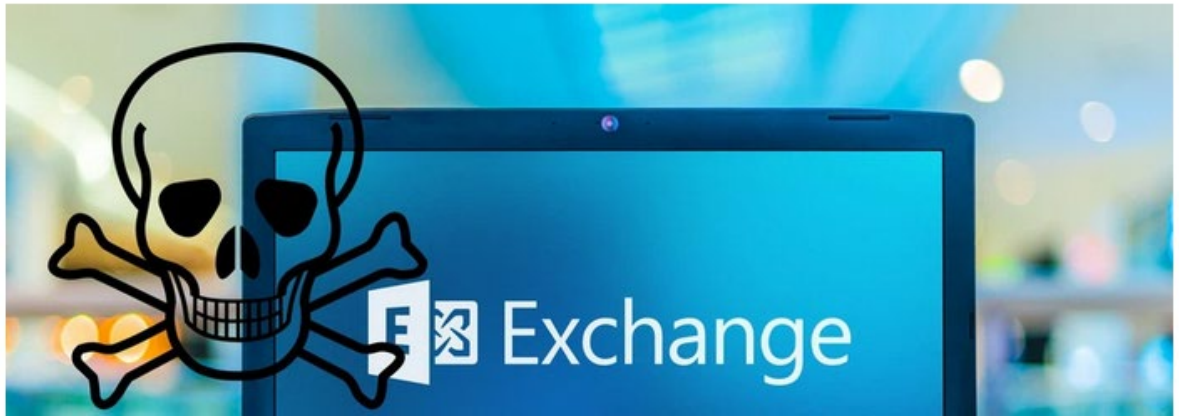
Wie das NCSC Informationen verwendet

- **Warnung:** Warnung vor aktuellen Cyberbedrohungen
- **Alarmierung:** Alarmierung bei Eintritt einer Cyberbedrohung

➢ Das NCSC liefert konkrete, technische und organisatorische Empfehlungen und unterstützt subsidiär bei der Vorfallsbewältigung («Incident Response»)

Wie das NCSC Informationen verwendet

watson 9° DE | FR



Über 130 Firmen und Gemeinden «verhängen» wichtige Updates – Bund warnt per Einschreiben

Das Nationale Zentrum für Cybersicherheit (NCSC) ruft IT-Verantwortliche von Gemeinden und in der Privatwirtschaft eindringlich dazu auf, Schwachstellen bei Exchange-Server-Software zu beheben.

Wie das NCSC Informationen verwendet

Lowend

17.02.2022 11:18 • registriert Februar 2014

Die Gemeinden machen keine wichtigen Updates ihrer IT-Systeme und der Bund warnt per Einschreiben. Das ist genau mein Humor, denn so wie ich den Bund kenne, wollten sie die Verantwortlichen sicher zuerst per Fax warnen, aber da war die Hälfte vermutlich unzustellbar. 🤣

34 20 Melden

...

So viel zur Digitalisierung der kantonalen Amtsstuben, Acronym und ja, das sind Amateure, denn diese Einstellung, per Einschreiben zu informieren ist so was von letztem Jahrhundert, wie auch die MS abhängige IT des Bundes, wo ich doch einige kenne.

7 11 Melden

Quelle: https://www.watson.ch/digital/schweiz/731746680-130-firmen-und-gemeinden-verschlampen-updates-warnung-per-einschreiben

Wie das NCSC Informationen verwendet

Wie das NCSC Informationen beschafft

- Herausforderungen bei der Benachrichtigung von Betroffenen:
  - Wie kann die betroffene Organisation hinter einer IP Adresse identifiziert werden?
  - Unternehmen ist in Liquidation, Postzustellung nicht möglich (… betreibt aber weiterhin IT-Infrastruktur)
  - Veraltete oder nicht korrekte Postanschrift (Internetanbieter, nic.ch, etc)

Wie das NCSC Informationen beschafft

- Wie der Briefversand im Jahr 2022 (nicht) funktioniert… [1/4]

NCSC MA:
«Grüäzi, ich hätte hier 500 Briefe zum Einschreiben»

Postangestellte/r:
«Tut mir leid, wir nehmen maximal 10 Briefe pro Sendung an»

NCSC Mitarbeiter radelt mit dem Velo in die Nachbarsgemeinden…

Wie das NCSC Informationen beschafft

- Wie der Briefversand im Jahr 2022 (nicht) funktioniert… [2/4]

NCSC MA:
«Grüäzi, ich bräuchte 1’000 Einschreiben-Etiketten»

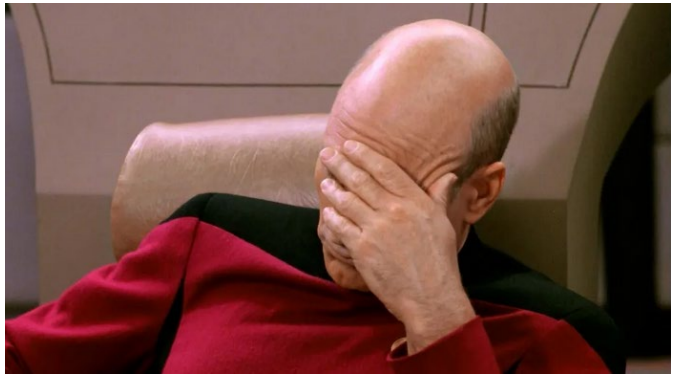
Postangestellte/r:
«So viele haben wir nicht. Wir können Ihnen aber 80 mitgeben»

NCSC Mitarbeiter radelt mit dem Velo (erneut) in die Nachbarsgemeinden…

Wie das NCSC Informationen beschafft

- Wie der Briefversand im Jahr 2022 (nicht) funktioniert… [3/4]

NCSC MA:
«Vorsicht! Sie haben eine Infektion in Ihrem Netzwerk, welche höchstwahrscheinlich zu einer Verschlüsselung mit Ransomware führt.»



Opfer:
«Annahme des Einschreiben verweigert»

Wie das NCSC Informationen beschafft

- Wie der Briefversand im Jahr 2022 (nicht) funktioniert… [4/4]

NCSC MA:
«Vorsicht! Sie haben eine Infektion in Ihrem Netzwerk, welche höchstwahrscheinlich zu einer Verschlüsselung mit Ransomware führt»

Opfer:
«Sendung nicht abgeholt, Abholfrist abgelaufen»

Vielen Dank für Ihre Aufmerksamkeit!

Roman Hüssy
Technischer Analytiker Cybersicherheit
roman.huessy@govcert.ch